Australasian Conf. on
Info Security & Privacy
24-26 June, 1996

International Security Harmonisation

Breakthroughs in Standardisation of IT Security Criteria

Eugene F. Troy

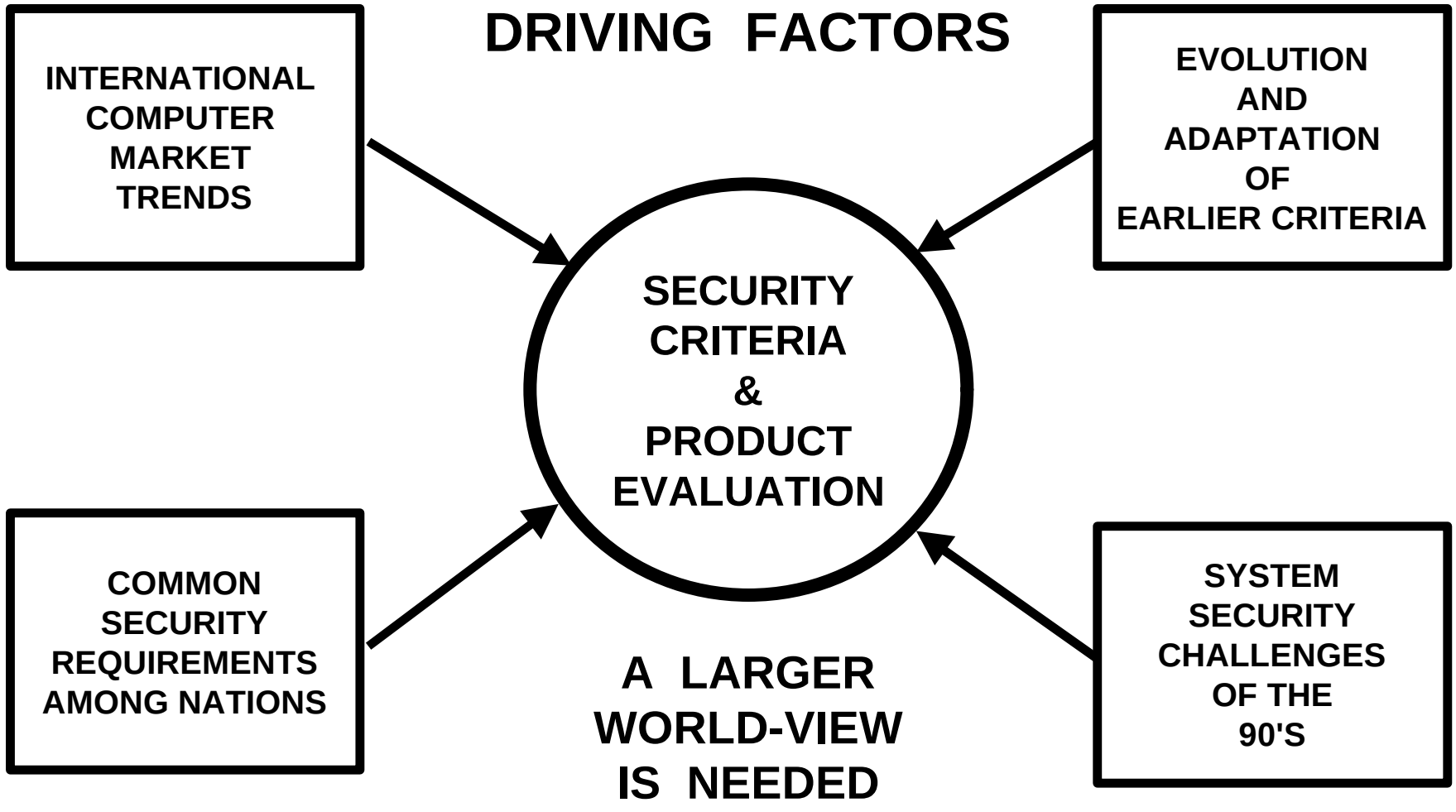
Project Manager, IT Security Criteria & Evaluations
National Institute of Standards and Technology
820 Diamond Avenue, MS: NN426
Gaithersburg, MD 20899 USA
voice: +1.301.975.3361, fax: +1.301.948.0279
eugene.troy@nist.gov

CCIB **Common Criteria Implementation Board**

Australasian Conf. on
Info Security & Privacy
24-26 June, 1996

The Common Criteria -- WHY DO IT?

DRIVING FACTORS

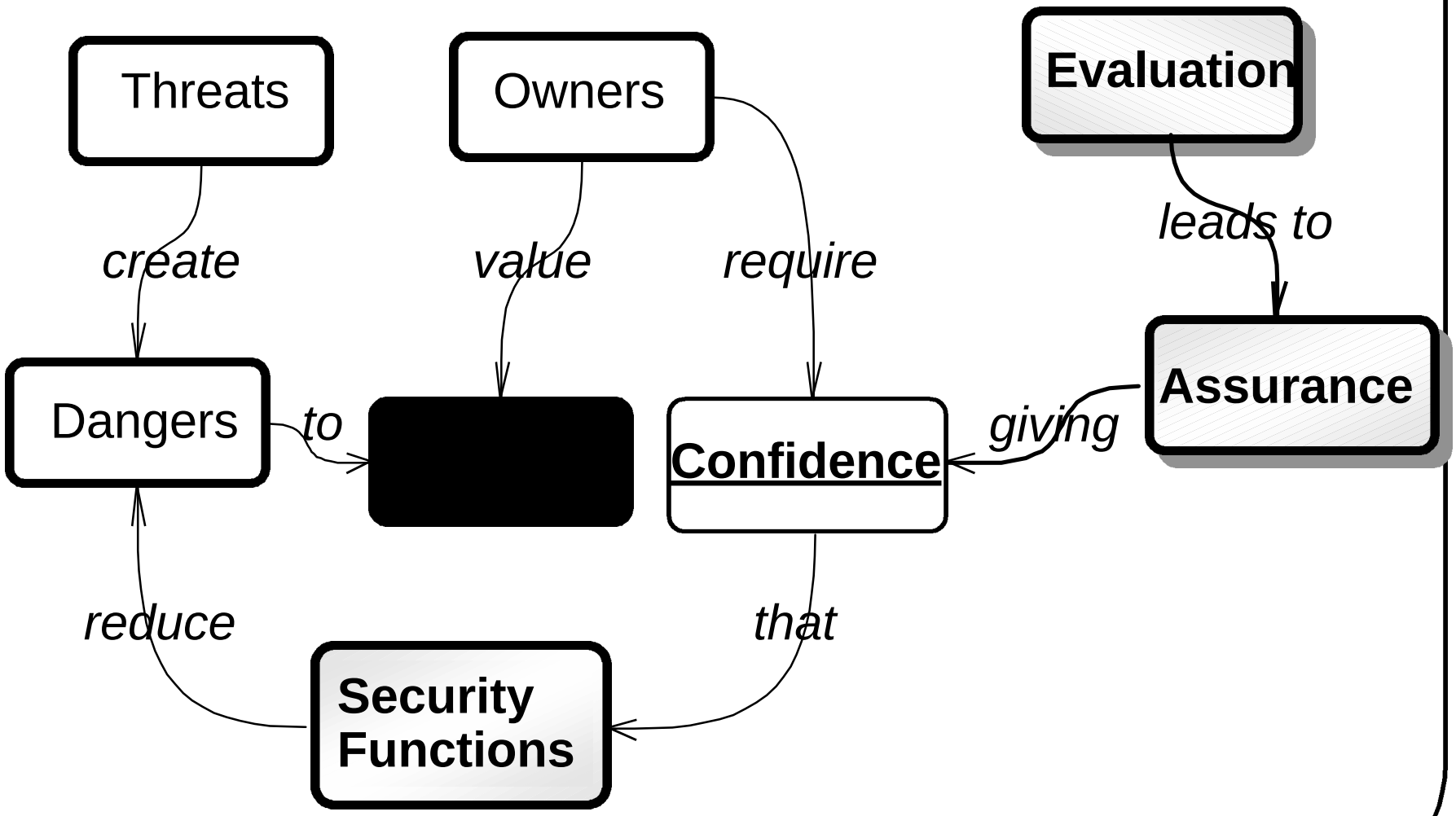


A LARGER WORLD-VIEW IS NEEDED

CCIB Common Criteria Implementation Board

Australasian Conf. on
Info Security & Privacy
24-26 June, 1996

Security Concepts and Relationships



Australasian Conf. on
Info Security & Privacy
24-26 June, 1996

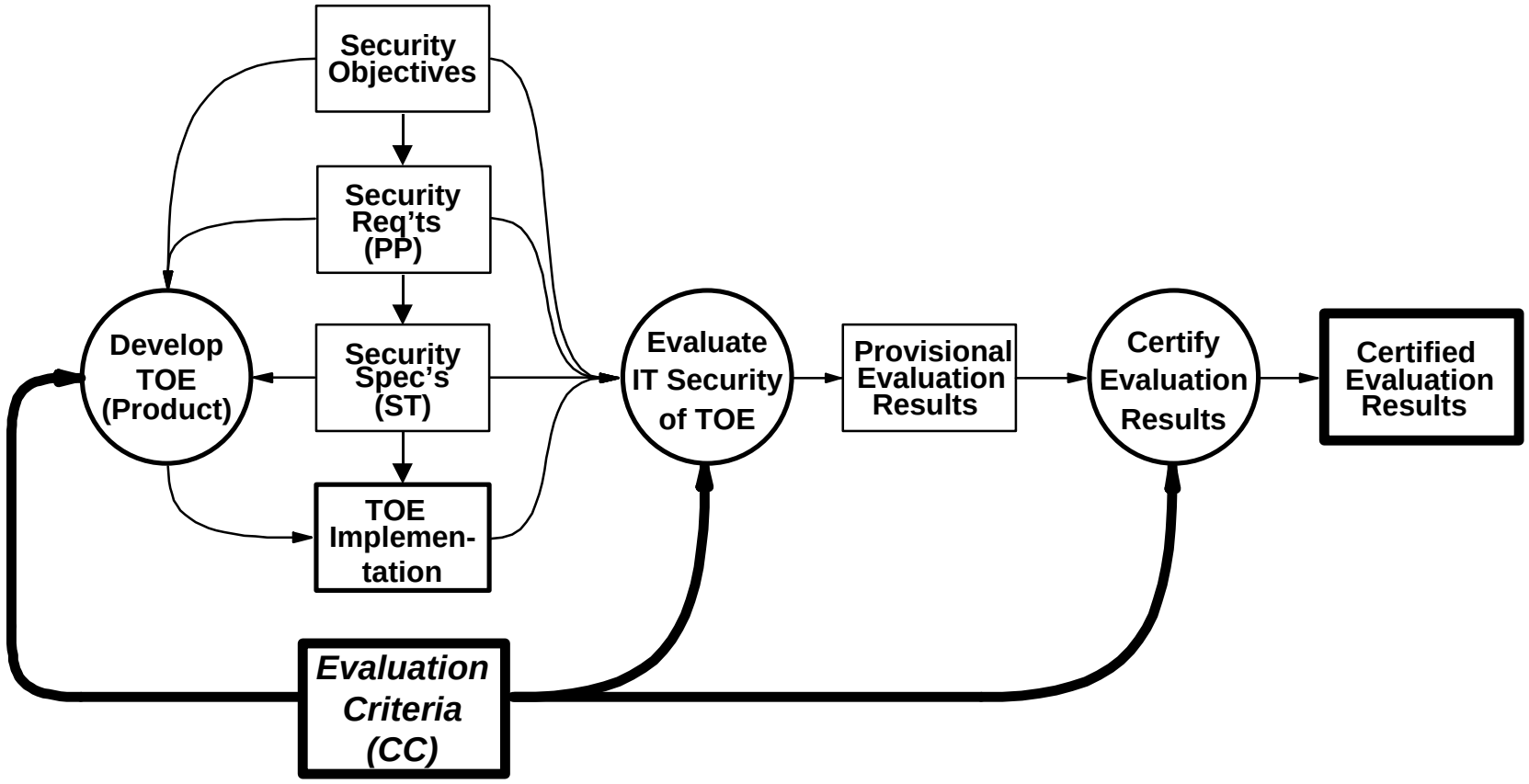
Twofold Purpose of IT Security Criteria

Well-Understood - Common & Solid Technical Basis for -->

- **Describing Product IT Security Requirements:**
  - **-- The Protection Profile (general), and Security Target (specific) (Part 1)**
  - **-- The Catalogue of Functional Requirement Components (Part 2)**
- **Deciding to Trust Security Functions in Products:**
  - **-- The Seven Evaluation Assurance Levels (EALs), plus...**
  - **-- The Catalogue of Assurance Requirement Components (Part 3)**

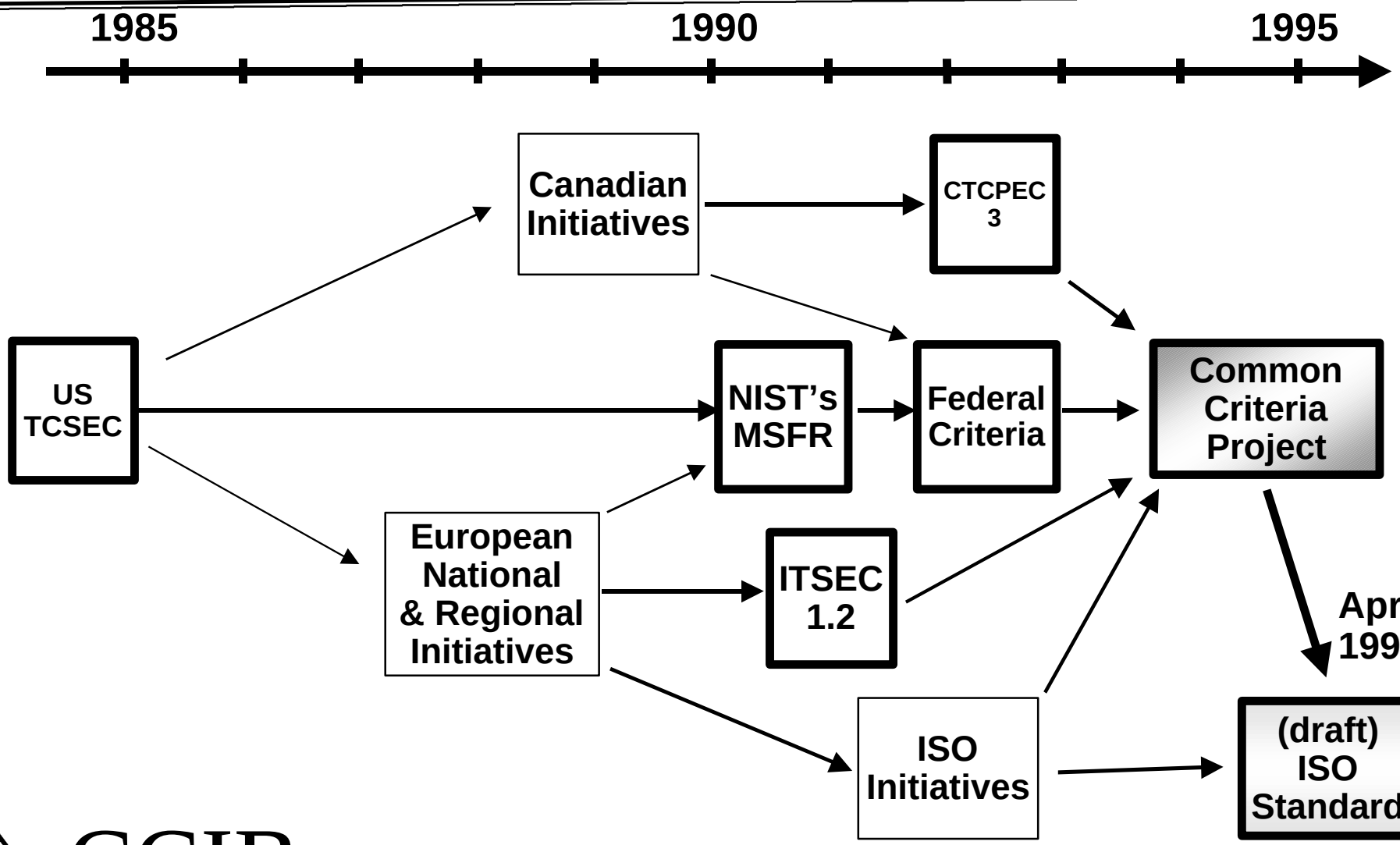
Australasian Conf. on
Info Security & Privacy
24-26 June, 1996

Context of IT Security Evaluations



Australasian Conf. on
Info Security & Privacy
24-26 June, 1996

A Brief History of IT Security Criteria



CCIB Common Criteria Implementation Board

Australasian Conf. on
Info Security & Privacy
24-26 June, 1996

Common Criteria Project Participants

- **North America:**
  - *Canada* Communications Security Establishment
  - *USA* National Institute of Standards & Technology
    National Security Agency
- **Europe:**
  - *France* Central Service for Info. Systems Security
  - *Germany* German Information Security Agency
  - *Netherlands* -- National Communications Security Agency
  - *UK* Communications-Electronics Security Group

Australasian Conf. on
Info Security & Privacy
24-26 June, 1996

Overview of Common Criteria v1.0 Structure

Part 3 Security Assurance Requirements

- Assurance Classes
- Assurance Families
- Assurance Components
- Detailed Req'ts
- Eval. Assur. Levels

Part 2 Security Functional Requirements

- Functional Classes
- Functional Families
- Functional Components
- Detailed Req'ts

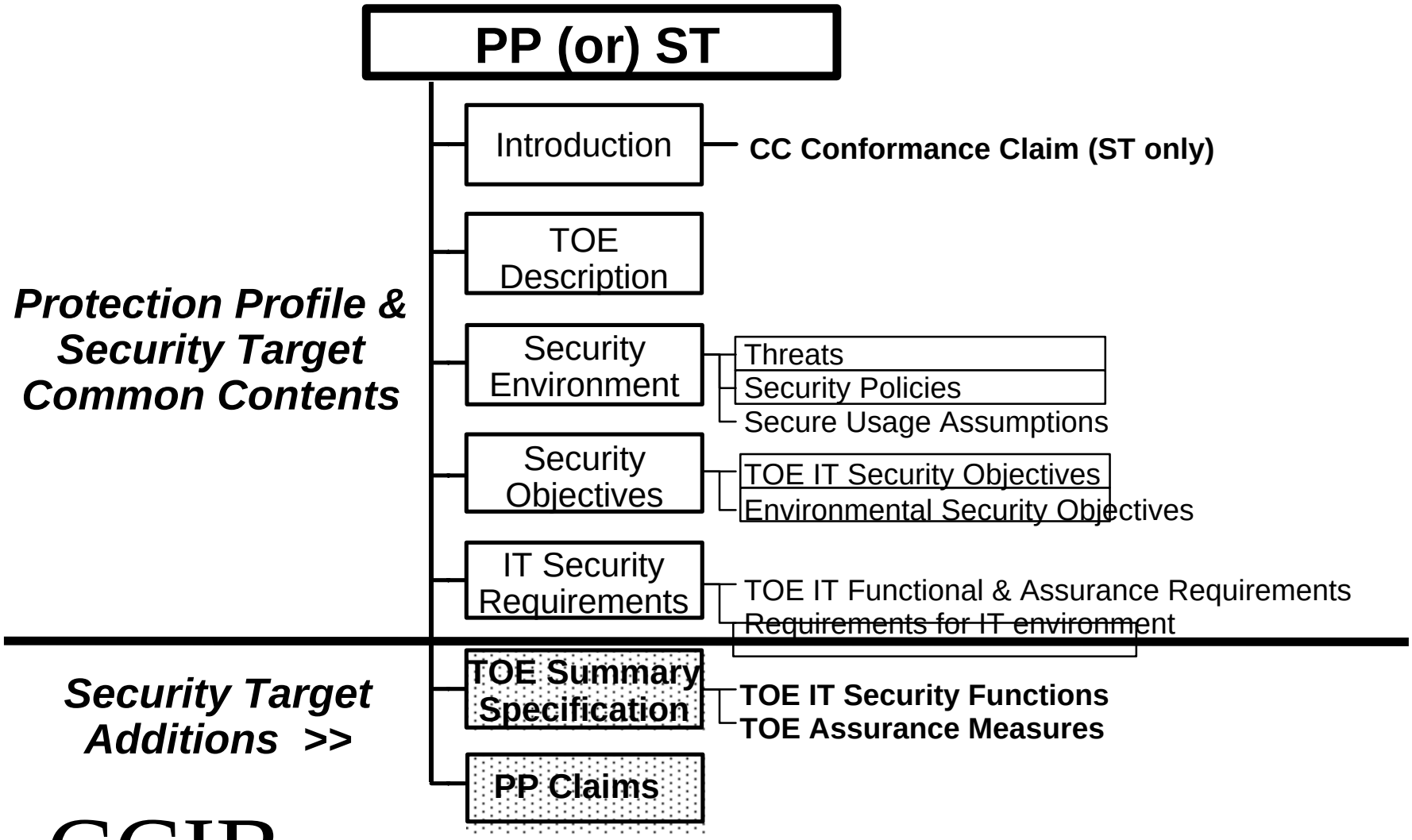
Part 1 Introduction & Model

- Introduction to Approach
- Terms & Model
- Requirements for Protection Profiles & Security Targets

Part 4 Registry of Protection Profiles

Australasian Conf. on
Info Security & Privacy
24-26 June, 1996

The Protection Profile & Security Target



CCIB Common Criteria Implementation Board

Australasian Conf. on
Info Security & Privacy
24-26 June, 1996

Part 2 -- Functional Security Requirements -- Classes

FAU -- Security Audit (35)

FCO -- Communication (Non-Repudiation) (4)

FCS -- Cryptographic Support *(in version 2)* (40)

FDP -- User Data Protection (46)

FIA -- Identification & Authentication (27)

FPR -- Privacy (Anonymity, etc.) (8)

FPT -- Protection of Trusted Security Functions (43)

FRU -- Resource Utilisation (8)

FTA -- TOE Access (11)

FTP -- Trusted Path (2)

NOTE:
Numbers in parentheses indicate the discrete callable components in each class - 224 in all.

Australasian Conf. on
Info Security & Privacy
24-26 June, 1996

The CC and Crypto (Draft "Technical Report")

"Crypto Caveat"

Criteria for assessment of mathematical properties of cryptographic algorithms and related techniques is not covered in the CC. (Part 1)

(Draft) Functional Class FCS: Cryptographic Support

- **Module Interface**
- **Roles and Services**
- **Physical Protection**
- **Secure Key: Generation, Distribution, Entry**
  Storage, Usage, Backup
  Output, Escrow, Archival, Destruction
- **Secure Cryptographic Function**
- **Self Integrity Tests**

(Draft) Assurance Class ADV: Development

- **Cryptographic Module Scope and Boundary**
- **Cryptographic Module Design**

NOTE:
Crypto support req'ts in draft come from US FIPS 140-1 & Canadian Crypto Annex.

Part 3 -- Assurance Requirements - *Classes*

ACM - Configuration Management

ADV - Development

ATE - Tests

AVA - Vulnerability Assessment

ADO - Delivery and Operation

AGD - Guidance Documents

ALC - Life-cycle Support

APE - Protection Profile Evaluation

ASE - Security Target Evaluation

Part 3 -- CC

Evaluation Assurance Levels (1)

Level EAL1 - (new)
The lowest level which should be considered for purposes of evaluation

Level EAL2 - (like C1 - E1)
The best that can be achieved without imposing some additional tasks on a developer

Level EAL3 - (like C2 - E2)
Allows a conscientious developer to benefit from positive security engineering design without alteration of existing reasonably sound development practices

Level EAL4 - (like B1 - E3)
The best that can be achieved without significant alteration of current good development practices.

CC

Evaluation Assurance Levels (2)

Level EAL5 - (like B2 - E4)
The best achievable via pre-planned, good quality, careful security-aware development without unduly expensive practices.

Level EAL6 - (like B3 - E5)
A "high tech" level for (mainly military) use in environments with *significant* threats and moderately valued assets.

Level EAL7 - (like A1 - E6)
The greatest amount of evaluation assurance attainable whilst remaining in the real world for real products.
EAL7 is at the limits of the current technology.

Part 4 -- Registry of Protection Profiles

Initial Goal:

Present ***Three*** "Example PPs" Written per CC Structure:
Two from Existing Criteria and One "New PP" --

-- CC/CS1 (C2) - Controlled Access OS

-- CC/CS3 - Role-Based Access OS

-- "Firewall" Packet Filtering Router

Ultimate Goal:

Be a "Living Catalog of PPs" -- the Registry for PPs
Which Have Completed the Registration Process

The Future

Trial-Use Period & Follow-On Tasks

- Do *Trial Evaluations* of Products
- Prepare *Evaluation Methods* Manual
- Negotiate *Mutual Recognition* Agreements
- Obtain Community Feedback via *Comments*
- Develop *Version 2*, Based on Experience / Feedback & Deliver to ISO SC27 Working Group 3
- Create *Implementing Guidance* (a la "Rainbow Series")
- Develop Part 5 -- *PP Registration* Procedures (with ISO SC27 Working Group 3)

SUMMARY

- **Developing Next Generation Criteria for IT Security**
- **Protecting Fundamental Principles of IT Security and Previous Investments in Technology**
- **Providing a Flexible and Extensible Framework for the Future**
- **Offering a Major Contribution to International Standards & Harmonisation**
- **Expected Result -- 'Level Playing Field' for IT-Security Products World-wide**